

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-101035

(43)Date of publication of application : 13.04.1999

(51)Int.Cl.

E05B 49/00
H04L 9/32

(21)Application number : 09-264138

(71)Applicant : PFU LTD

(22)Date of filing : 29.09.1997

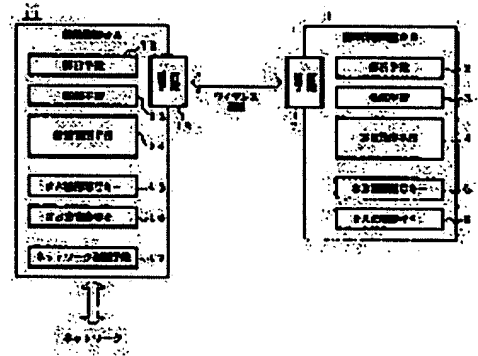
(72)Inventor : YAMAMOTO YOJI

(54) LOCK DEVICE SYSTEM AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To enhance safety by encoding/transmitting an individual locking code changing each time when a device ID is received from a portable terminal, and comparing it with former transmission data by again receiving/decoding an encoded signal from the portable terminal.

SOLUTION: Analyzing means 2 and 12 respectively analyze data transmitted from a lock device 11 and a portable information terminal 1. Secret code keys 5 and 15 and public code keys 6 and 16 respectively decode encoded data. When the portable information terminal 1 transmits a device proper ID, the lock device 11 confirms the ID, and encodes/transmits an individual locking code containing a time stamp changing each time by a public code key of the portable information terminal 1. Next, the portable information terminal 1 decodes a received signal, and encodes/transmits it again by the public code key of the lock device 11. The lock device 11 decodes the received signal, and discriminates whether or not it coincides with the former transmission content, and also discriminates whether or not the time stamp is within a prescribed time. Therefore, safety is enhanced, and a lock can be set and opened.



LEGAL STATUS

[Date of request for examination] 22.01.2001

[Date of sending the examiner's decision of rejection] 11.05.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-101035

(43)公開日 平成11年(1999) 4月13日

(51)Int.Cl.⁶

E 0 5 B 49/00

H 0 4 L 9/32

識別記号

F I

E 0 5 B 49/00

H 0 4 L 9/00

K

6 7 3 B

6 7 5 B

審査請求 未請求 請求項の数 8 O L (全 11 頁)

(21)出願番号

特願平9-264138

(22)出願日

平成9年(1997)9月29日

(71)出願人 000136136

株式会社ピーエフユー

石川県河北郡宇ノ気町宇野気ヌ98番地の
2

(72)発明者 山本 洋史

石川県河北郡宇ノ気町宇野気ヌ98番地の
2 株式会社ピーエフユー内

(74)代理人 弁理士 岡田 守弘

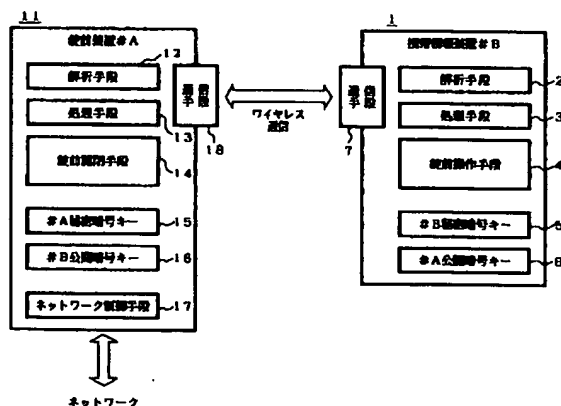
(54)【発明の名称】 錠前装置システムおよび記録媒体

(57)【要約】

【課題】 本発明は、錠前を施錠あるいは開錠する錠前装置システムおよび記録媒体に関し、錠前装置と操作作用の携帯情報装置との間で暗号化技術を使って安全性を高めることを目的とする。

【解決手段】 自装置の装置IDを施錠装置に送信する手段と、送信に対応して施錠装置から返信されてきたデータについて自装置の秘密暗号キーで復号した後、錠前装置の公開暗号キーで暗号化して送信する手段とからなる装置と、装置から受信した装置IDが予め登録されていた装置IDと一致したときに装置IDと一緒に登録されている装置の公開暗号キーを用いて毎回変化する個別施錠コードを暗号化して上記装置に返信する手段と、返信したことに対応して装置から送信されてきたデータを錠前装置の秘密暗号キーで復号したデータと個別施錠コードとが一致したときに指定された施錠あるいは開錠を行う手段とからなる施錠装置とを備えた錠前装置システムである。

本発明のシステム構成図



【特許請求の範囲】

【請求項 1】錠前を施錠あるいは開錠する錠前装置システムにおいて、

自装置の装置 ID を施錠装置に送信する手段と、上記送信に対応して施錠装置から返信されてきたデータについて自装置の秘密暗号キーで復号した後、錠前装置の公開暗号キーで暗号化して送信する手段とからなる装置と、上記装置から受信した装置 ID が予め登録されていた装置 ID と一致したときに装置 ID に一緒に登録されている装置の公開暗号キーを用いて毎回変化する個別施錠コードを暗号化して上記装置に返信する手段と、上記返信したことに対応して上記装置から送信されてきたデータを錠前装置の秘密暗号キーで復号したデータと上記個別施錠コードとが一致したときに指定された施錠あるいは開錠を行う手段とからなる施錠装置とを備えた錠前装置システム。

【請求項 2】上記毎回変化する個別施錠コードとして、時刻あるいは時刻と乱数でランダムに作成したコードを組み合わせた情報としたことを特徴とする請求項 1 記載の施錠装置システム。

【請求項 3】上記復号したデータと上記個別施錠コードとが一致し、かつ当該個別施錠コード中の時刻と現時刻との差が所定時間以内のときに指定された施錠あるいは開錠を行うことを特徴とする請求項 1 あるいは請求 2 記載の施錠装置システム。

【請求項 4】自装置の公開暗号キーおよび錠前装置 ID を管理装置に送信する手段と、錠前装置から送信されてきたデータを自装置の秘密暗号キーを用いて復号化した錠前装置の公開暗号キーを登録する手段とを設けた装置と、

上記装置から送信されてきた装置の公開暗号キーおよび錠前装置 ID と当該錠前装置 ID のキー登録プログラムを錠前装置 ID の公開暗号キーで暗号化して錠前装置に送信する手段を設けた管理装置と、

上記管理装置から送信されてきたデータを自身の秘密暗号キーで復号化したキー登録プログラムおよび装置の公開暗号キーを登録する手段と、登録した装置の公開暗号キーを用いて自錠前装置の公開暗号キーを暗号化して上記装置に送信する手段とを設けた錠前装置とを備え、続いて請求項 1 ないし請求項 3 記載のいずれかの処理を実行することを特徴とする錠前装置システム。

【請求項 5】自装置の公開暗号キーを錠前装置に送信する手段と、錠前装置から送信されてきたデータを自装置の秘密暗号キーを用いて復号化して錠前装置の公開暗号キーを登録する手段とを設けた装置と、

上記装置から送信されてきた装置の公開暗号キーを登録すると共に当該公開暗号キーを用いて自錠前装置の公開暗号キーを暗号化して上記装置に送信する手段とを設けた錠前装置とを備え、続いて請求項 1 ないし請求項 3 記載のいずれかの処理を実行することを特徴とする錠前装

置システム。

【請求項 6】上記登録した公開暗号キーに使用回数あるいは使用期間の制限を付与して当該制限を越えたときに自己消滅するプログラムを付与したことを特徴とする請求項 4 あるいは請求項 5 記載の錠前装置システム。

【請求項 7】錠前装置の施錠したときに当該錠前装置の公開暗号キーを用いて錠前開閉制御プログラムを暗号化した後に装置の公開暗号キーを用いて暗号化して装置に送信すると共に錠前開閉制御プログラムを消去する手段と、開錠するときに装置から送信されてきたデータを自錠前装置の秘密暗号キーを用いて復号した錠前開閉制御プログラムをインストールして開錠する手段とを設けた錠前装置と、

上記施錠したときに錠前装置から送信されてきたデータを保持する手段と、開錠するときに上記保持したデータを自装置の秘密暗号キーを用いて復号して上記錠前装置に送信する手段とを設けた装置とを備え、上記施錠および開錠の直前に請求項 1 ないし請求項 3 記載のいずれかの処理をそれぞれ実行することを特徴とする錠前装置システム。

【請求項 8】コンピュータを動作させ、自装置の装置 ID を施錠装置に送信する手段と、上記送信に対応して施錠装置から返信されてきたデータについて自装置の秘密暗号キーで復号した後、錠前装置の公開暗号キーで暗号化して送信する手段として機能させる、装置に格納するプログラムと、

上記装置から受信した装置 ID が予め登録されていた装置 ID と一致したときに装置 ID に一緒に登録されている装置の公開暗号キーを用いて毎回変化する個別施錠コードを暗号化して上記装置に返信する手段と、上記返信したことに対応して上記装置から送信されてきたデータを錠前装置の秘密暗号キーで復号したデータと上記個別施錠コードとが一致したときに指定された施錠あるいは開錠を行う手段として機能させる、施錠装置に格納するプログラムとのいずれか、あるいは両者を記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、錠前を施錠あるいは開錠する錠前装置システムおよび記録媒体に関するものである。

【0002】

【従来の技術】従来、キーレスエントリと称して、ワイヤレス通信による錠前機構が数多く提供されるようになった。

【0003】

【発明が解決しようとする課題】しかし、従来の装置では、ワイヤレス通信情報を傍受された場合に錠前としての安全性に欠けるという問題があった。

【0004】本発明は、これらの問題を解決するため、

錠前装置と操作の携帯情報装置との間で暗号化技術を使って安全性を高めることを目的としている。

【0005】

【課題を解決するための手段】図1を参照して課題を解決するための手段を説明する。図1において、携帯端末装置（装置）1は、秘密暗号キーおよび公開暗号キーを用いて錠前装置11の施錠あるいは開錠を行うものである。

【0006】錠前装置11は、秘密暗号キーおよび公開暗号キーを用いて装置1との間でデータの送受信して錠前を施錠あるいは開錠するものである。次に、動作を説明する。

【0007】装置（携帯情報装置）1が自装置の装置IDを施錠装置11に送信し、施錠装置11が受信した装置IDについて予め登録されていた装置IDと一致したときに装置IDと一緒に登録されている装置の公開暗号キーを用いて毎回変化する個別施錠コードを暗号化して装置1に返信し、装置1が返信されてきたデータについて自装置の秘密暗号キーで復号した後に、錠前装置の公開暗号キーで暗号化して送信し、錠前装置11が送信されてきたデータを錠前装置の秘密暗号キーで復号したデータと個別施錠コードとが一致したときに指定された施錠あるいは開錠を行うようにしている（処理（A）とする）。

【0008】この際、毎回変化する個別施錠コードとして、時刻あるいは時刻と乱数でランダムに作成したコードを組み合わせた情報とするようにしている。また、復号したデータと個別施錠コードとが一致し、かつ個別施錠コード中の時刻と現時刻との差が所定時間以内のときに指定された施錠あるいは開錠を行うようにしている。

【0009】また、装置1が管理装置に公開暗号キーおよび錠前装置IDを送信し、管理装置が送信されてきた装置の公開暗号キーおよび錠前装置IDと錠前装置IDのキー登録プログラムを錠前装置IDの公開暗号キーで暗号化して錠前装置11に送信し、錠前装置11が送信されてきたデータを自身の秘密暗号キーで復号化したキー登録プログラムおよび装置の公開暗号キーを登録すると共に登録した装置の公開暗号キーを用いて自錠前装置の公開暗号キーを暗号化して装置1に送信し、装置1が送信されてきたデータを自装置の秘密暗号キーを用いて復号化して錠前装置の公開暗号キーを登録するようにしている。そして、上記処理（A）を実行するようにしている。

【0010】また、装置1が自装置の公開暗号キーを錠前装置11に送信し、錠前装置11が送信されてきた装置の公開暗号キーを登録すると共に公開暗号キーを用いて自錠前装置の公開暗号キーを暗号化して装置1に送信し、装置1が送信されてきたデータを自装置の秘密暗号キーを用いて復号化して錠前装置の公開暗号キーを登録するようにしている。そして、上記処理（A）を実行す

るようにしている。

【0011】この際、登録した公開暗号キーに使用回数あるいは使用期間の制限を付与して制限を越えたときに自己消滅するプログラムを付与するようにしている。また、錠前装置11が施錠したときに錠前装置の公開暗号キーを用いて錠前開閉制御プログラムを暗号化した後に装置の公開暗号キーを用いて暗号化して装置1に送信すると共に錠前開閉制御プログラムを消去し、装置1が送信されてきたデータを保持し、開錠するときに保持したデータを自装置の秘密暗号キーを用いて復号して錠前装置11に送信し、錠前装置11が送信されてきたデータを自錠前装置の秘密暗号キーを用いて復号した錠前開閉制御プログラムをインストールして開錠するようにしている。この際、施錠および開錠の直前に上記処理（A）を実行するようにしている。

【0012】従って、錠前装置11と装置（携帯情報端末）1との間で暗号化技術を使って安全性を高めて、錠前装置11の施錠あるいは開錠を行うことが可能となる。

【0013】

【発明の実施の形態】次に、図1から図5を用いて本発明の実施の形態および動作を順次詳細に説明する。

【0014】図1は、本発明のシステム構成図を示す。ここで、図示外の記録媒体あるいは外部記憶装置であるハードディスク装置から読み出したプログラム、またはセンタのはハードディスク装置から回線を介して転送されてきたプログラムを主記憶にローディングして起動し、以下に説明する各種処理を行うものである。

【0015】図1において、携帯情報装置（装置）1は、ここでは以下の説明を簡単にするために装置1と記載し、施錠装置11の施錠あるいは開錠を暗号技術（秘密暗号キーおよび公開暗号キーを用いた例えば公知のDES技術）を用いて行うものであって、解析手段2、処理手段3、錠前操作手段4、秘密暗号キー5、公開暗号キー6などから構成されるものである。

【0016】解析手段2は、錠前装置11などから送信されてきたデータを解析し、該当する処理を実行させるものである。処理手段3は、解析手段2によって解析された結果をもとに各種処理を行うものである。

【0017】錠前操作手段4は、錠前を施錠あるいは開錠操作などを指示するものである。秘密暗号キー5および公開暗号キー6は、DES技術などで用いる秘密暗号キーおよび公開暗号キーであって、秘密暗号キーを用いて暗号化されたデータは公開暗号キーで復号化でき、逆に公開暗号キーを用いて暗号化されたデータは秘密暗号キーで復号化できるという性質を持つものである。

【0018】通信手段7は、ワイヤレス通信で施錠装置11との間でデータの送受信を行うものである。施錠装置11は、図示外の錠前を施錠したり開錠したりなどするものであって、解析手段2、処理手段3、錠前開閉手

段4、秘密暗号キー15、公開暗号キー16、ネットワーク制御手段17、および通信手段18などから構成されるものである。

【0019】解析手段12は、携帯情報装置1などから送信されてきたデータを解析し、該当する処理を実行させるものである。処理手段13は、解析手段12によって解析された結果をもとに各種処理を行うものである。

【0020】錠前開閉手段14は、錠前を施錠あるいは開錠したりするものであって、キー登録プログラムによって実行するものである。秘密暗号キー15および公開暗号キー16は、DES技術などで用いる秘密暗号キーおよび公開暗号キーであって、秘密暗号キーを用いて暗号化されたデータは公開暗号キーで復号化でき、逆に公開暗号キーを用いて暗号化されたデータは秘密暗号キーで復号化できるという性質を持つものである。

【0021】ネットワーク制御手段17は、ネットワークを介して管理装置や他の携帯情報装置1との間でデータの授受を行うものである。通信手段18は、ワイヤレス通信で携帯情報装置1との間でデータの送受信を行うものである。

【0022】次に、図2のフローチャートに示す順序に従い図1の構成の動作を詳細に説明する。図2は、本発明の動作説明フローチャート(その1)を示す。ここで、携帯情報端末1を#B、錠前装置11を#Aと説明を簡単にするために記述する。

【0023】図2において、S1は、携帯情報端末1が錠前の操作を開始し、#B(携帯情報端末1を表す)の装置固有IDを送信する。S2は、錠前装置11がS1で送信されたデータを受信し、受信したIDの装置の公開暗号キーが#A(錠前装置11を表す)内に登録されているか確認する。

【0024】S3は、登録されているか判別する。YESの場合には、S4に進む。NOの場合には、登録されていないと判明したので、エラーとして終了する。S4は、#Bの公開暗号キーで毎回変化する個別施錠コード(タイムスタンプを含む)情報を暗号化する。これは、毎回変化する個別施錠コードとして、現在の時刻を用い、これを暗号化する。

【0025】S5は、S4で暗号化した情報(データ)を送信する。S6は、S5で送信された情報を受信する。S7は、#B秘密暗号キーで受信情報を復号化する。これにより、S4で暗号化した元の個別施錠コードが復号されたこととなる。

【0026】S8は、復号した情報を#A公開暗号キーで暗号化する。これは、S7で復号された個別施錠コードを、#A公開暗号キー(施錠装置11の公開暗号キー)で暗号化する。

【0027】S9は、S8で暗号化した情報を送信する。S10は、S9で送信された情報を受信する。S11は、#A秘密暗号キーで受信情報を復号化し、元の個

別施錠コードを復号する。

【0028】S12は、送信内容と一致か判別する。これは、S11で受信情報を復号した情報(元の個別施錠コード)と、S4の個別施錠コードとが一致するか判別する。YESの場合には、#Bの認証がOKとしてS13で、更にタイムスタンプが所定時間以内か判別する。これは、S11で復号化したときに含まれているS4で含ませたタイムスタンプと現在の時刻とを比較し、その差が所定時間以内か判別する。YESの場合には、所定時間以内で正当性が高いとしてS14に進む。NOの場合には、正当性が低いとして施錠/開錠を認めず、終了する。

【0029】S14は、施錠状態か判別する。YESの場合には、S15で開錠し、終了する。NOの場合には、S16で施錠し、終了する。以上によって、装置#Bが装置固有IDを施錠装置#Aに送信し、施錠装置#Aが装置#Bの公開暗号キーで個別施錠コードとタイムスタンプを暗号化して装置#Bに送信し、装置#Bが装置#Bの秘密暗号キーで復号し、復号した情報を施錠装置#Aの公開暗号キーで暗号化して送信し、施錠装置#Aが施錠装置#Aの秘密暗号キーで復号化して個別施錠コードと一致したときに、更に復号化したタイムスタンプの経過時刻が所定時間以内のときに装置#Bの認証OKとし、施錠あるいは開錠を行うことにより、装置#Bと施錠装置#Aが暗号技術を用いて相互に通信して施錠装置#Aが装置#Bの認証OKとなったときに初めて施錠あるいは開錠を行い、暗号技術を合理的に使い安全性を高めることが可能となった。ここで、S1からS16(あるいはS1からS13)までの処理を処理(A)としてこれを基本動作と記述し、後述する図3、図4、図5で該当する個所で実行する。

【0030】図3は、本発明の動作説明フローチャート(その2)を示す。ここで、携帯情報端末1を#C、錠前装置11を#Aと説明を簡単にするために記述する。図3において、S21は、錠前装置#Aを使いたいとし、#C公開暗号キーを管理者へ渡す(あるいは送信する)。

【0031】S22は、錠前装置#A管理者(管理装置)が#Aのキー登録プログラム、#C公開暗号キー、#A使用許可回数/期間をバックにした情報を、#A公開暗号キーで暗号化する。

【0032】S23は、暗号化情報をネットワーク経由で錠前装置#Aに送信する。S24は、錠前装置#AがS23で送信された情報を受信する。S25は、#A秘密暗号キーで復号化する。

【0033】S26は、復号化した#Aのキー登録プログラムを起動する。S27は、指定された利用回数/利用期間条件を持ち、#Aに#C公開暗号キーが登録される。これにより、錠前装置#Aには、利用回数/利用期間条件を付与した装置#Cの公開暗号キーが登録される

10

20

30

40

50

こととなる。

【0034】S28は、#C公開暗号キーにより#A公開暗号キーを暗号化して#Cに送信する。S29は、S28で送信された情報を、装置#Cが受信する。

【0035】S30は、S29で受信した情報を、#C秘密暗号キーで復号化する。これにより、施錠装置#Aの公開暗号キーが復号されることとなる。S31は、#A公開暗号キーを装置に登録する。

【0036】S32は、基本動作と同様に施錠操作を行う（既述した図2のS1ないしS16で装置#Cの認証および施錠／開錠を行う）。また、S33は、施錠装置#Aが図2の既述した基本動作と同様に施錠動作をS32に対応して行う。

【0037】S34は、使用回数／期限を越えたか判別する。YESの場合には、S35で登録されている#C公開暗号キーの登録を抹消し、以降施錠／開錠できないようにし、もし盗用されてもいつまでも継続されることを防止することが可能となる。一方、S34のNOの場合には、S33で戻り繰り返す。

【0038】以上によって、装置#Cが自身の公開暗号キーおよび操作したい施錠装置#Aを管理装置（管理者）に通知し、管理装置（管理者）がキー登録プログラム、#C公開暗号キー、使用回数／期間を暗号化して施錠装置#Aに送信し、施錠装置#Aがキー登録プログラムを起動し、指定された使用回数／期間を付与した#C公開暗号キーを登録すると共に、#C公開暗号キーで#A公開暗号キーを暗号化した送信し、装置#Cが#C秘密暗号キーで復号し、復号した#A公開暗号キーを登録し、基本動作（既述した図2のS1からS16）により施錠あるいは開錠を行うことが可能となる。そして、施錠装置#Aに登録した#C公開暗号キーに付与されている使用回数／期限が越えたときに抹消し、再登録を促し、継続した盗用を防止することが可能となる。

【0039】図4は、本発明の動作説明フローチャート（その3）を示す。ここで、携帯情報端末1を#D、錠前装置11を#Aと説明を簡単にするために記述する。図4において、S41は、携帯情報端末1が錠前の操作を開始し、#D公開暗号キーを送信する。

【0040】S42は、錠前装置11がS41で送信された#D公開暗号キーを受信する。S43は、未登録装置の操作許可モードか判別する。YESの場合には、S44に進む。NOの場合には、終了する。

【0041】S44は、一定の条件（使用回数／期限）により自己消滅するプログラムを内包した#A公開暗号キーを#D公開暗号キーで暗号化する。S45は、暗号化した情報を送信する。

【0042】S46は、S45で送信された情報を、装置#Dが受信する。S47は、#D秘密暗号キーで受信情報を復号化する。これにより、S44で暗号化した元のプログラムを内包した#A公開暗号キーを復元でき

る。

【0043】S48は、復号した#A公開暗号キーを登録する。S49は、基本動作と同様に施錠操作する。これは、既述した図2のS1、S6ないしS9を実行する。そして、S50に進む。

【0044】S50は、使用回数／期限を越えたか判別する。YESの場合には、S51で#A公開暗号キーが内包されているプログラムにより自己消滅し、終了する。NOの場合には、S49を繰り返し、施錠あるいは開錠を繰り返す。

【0045】また、S52は、施錠装置#Aが#D公開暗号キーを使用回数／期限条件付きで登録する。S53は、基本動作と同様に施錠動作する。これは、既述した図2のS2ないしS5、S10からS16を実行する。そして、S54に進む。

【0046】S54は、使用回数／期限を越えたか判別する。YESの場合には、S55で#D公開暗号キーを内包するプログラムが登録を抹消し、終了する。NOの場合には、S53を繰り返し、施錠あるいは開錠を繰り返す。

【0047】以上によって、装置#Dが#D公開暗号キーを施錠装置#Aに送信し、施錠装置#Aが装置#Dの公開暗号キーで使用回数／期限付きで消滅するプログラムを内包させた#A公開暗号キーを暗号化して送信し、装置#Dが装置#Dの秘密暗号キーで復号し、復号した#A公開暗号キーを登録し、図2で既述したようにして施錠あるいは開錠を行い、登録した公開暗号キー使用回数／期限を越えたときに自動消滅させ、再登録を促し、安全性を高めることが可能となる。

【0048】図5は、本発明の動作説明フローチャート（その4）を示す。ここで、携帯情報端末1を#B、錠前装置11を#Aと説明を簡単にするために記述する。図5において、S61は、基本動作の（A）までの動作（図2のS1ないしS13）までの動作を実行する。

【0049】S62は、施錠状態か判別する。YESの場合には、施錠状態であるため終了する。NOの場合には、S63に進む。S63は、施錠する。

【0050】S64は、施錠装置の開閉制御プログラムをまず#A公開暗号キーで暗号化後、その情報をさらに#B公開暗号キーで暗号化する。S65は、暗号化した情報を送信する。そして、S65'で錠前装置の開閉制御プログラムを消去する。

【0051】S66は、S65で送信された情報を、装置#Bが受信し、受信情報Pを保持する。S67は、装置#Bが錠を開錠したいと指定する。

【0052】S68は、S61と同様に、基本動作の（A）までの動作（図2のS1ないしS13）までの動作を実行する。S69は、錠前装置#Aが情報Pの送信要求を通知する。

【0053】S70は、装置#Bが要求を受信の後、情

10

20

30

40

50

報Pを#B秘密暗号キーで復号化し、S64で#A秘密暗号キーで暗号化された情報に戻す。S71は、S70で復号化した情報P'を送信する。そして、S75で情報P(P')を消去する。

【0054】S72は、錠前装置#AがS71で送信された情報P'を受信し、#A秘密暗号キーで復号し、元の開閉制御プログラムに戻す。S73は、復号化した錠前機構制御プログラムを装置にインストールする。これにより、S65'で消去した錠前装置の開閉制御プログラムが復元されたこととなる。

【0055】S74は、開錠する。以上によって、装置#Bが施錠装置#Aを施錠した後、施錠装置#Aが開閉制御プログラムを#A公開暗号キーで暗号化し、更に#B公開暗号キーで二重に暗号化した装置#Dに送信し、装置#Dが情報Pを保持する。そして、開錠時に、保持した情報Pを装置#Dが秘密暗号キーで復号してこれを施錠装置#Dに送信し、施錠装置#Dが秘密暗号キーで復号して元の開閉制御プログラムに戻し、インストールして開錠を行うことにより、施錠時に錠前装置#Dに開閉制御プログラムを抹消し、開錠時に装置#Dが秘密暗号キーで復号して施錠装置#Dに送信しこれを更に秘密暗号キーで復号して元の開閉制御プログラムに戻してインストールして開錠し、安全性を決めた高くすることが可能となる。

【0056】

【発明の効果】以上説明したように、本発明によれば、錠前装置11と装置1との間で秘密暗号キーおよび公開暗号キーを使って情報や開閉制御プログラムのやり取り

を行い、装置1の認証を行った後に施錠あるいは開錠を行う構成を採用しているため、安全性を高めて錠前装置11の施錠あるいは開錠を行うことができると共に、登録した公開暗号キーに使用回数/期限の制限を付与してこれを越えたときに抹消し、再登録を促し、更に安全性を高めることができる。

【図面の簡単な説明】

【図1】本発明のシステム構成図である。

10 【図2】本発明の動作説明フローチャート(その1)である。

【図3】本発明の動作説明フローチャート(その2)である。

【図4】本発明の動作説明フローチャート(その3)である。

【図5】本発明の動作説明フローチャート(その4)である。

【符号の説明】

1：装置(携帯情報装置)

2、12：解析手段

20 3、13：処理手段

4：錠前操作手段

5、15：秘密暗号キー

6、16：公開暗号キー

7、18：通信手段

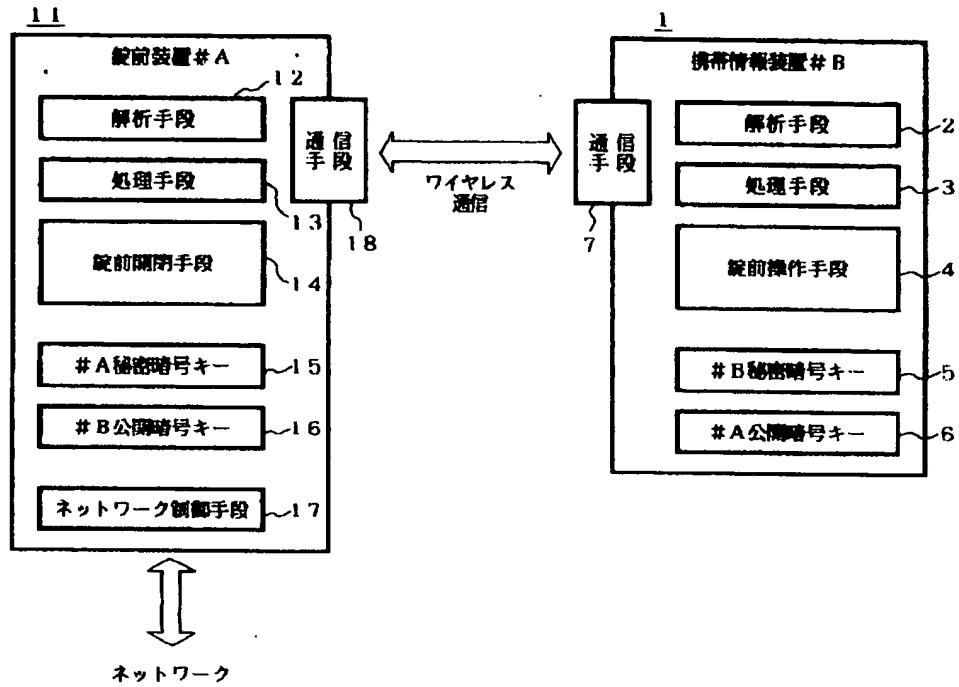
11：錠前装置

14：錠前開閉手段

17：ネットワーク制御手段

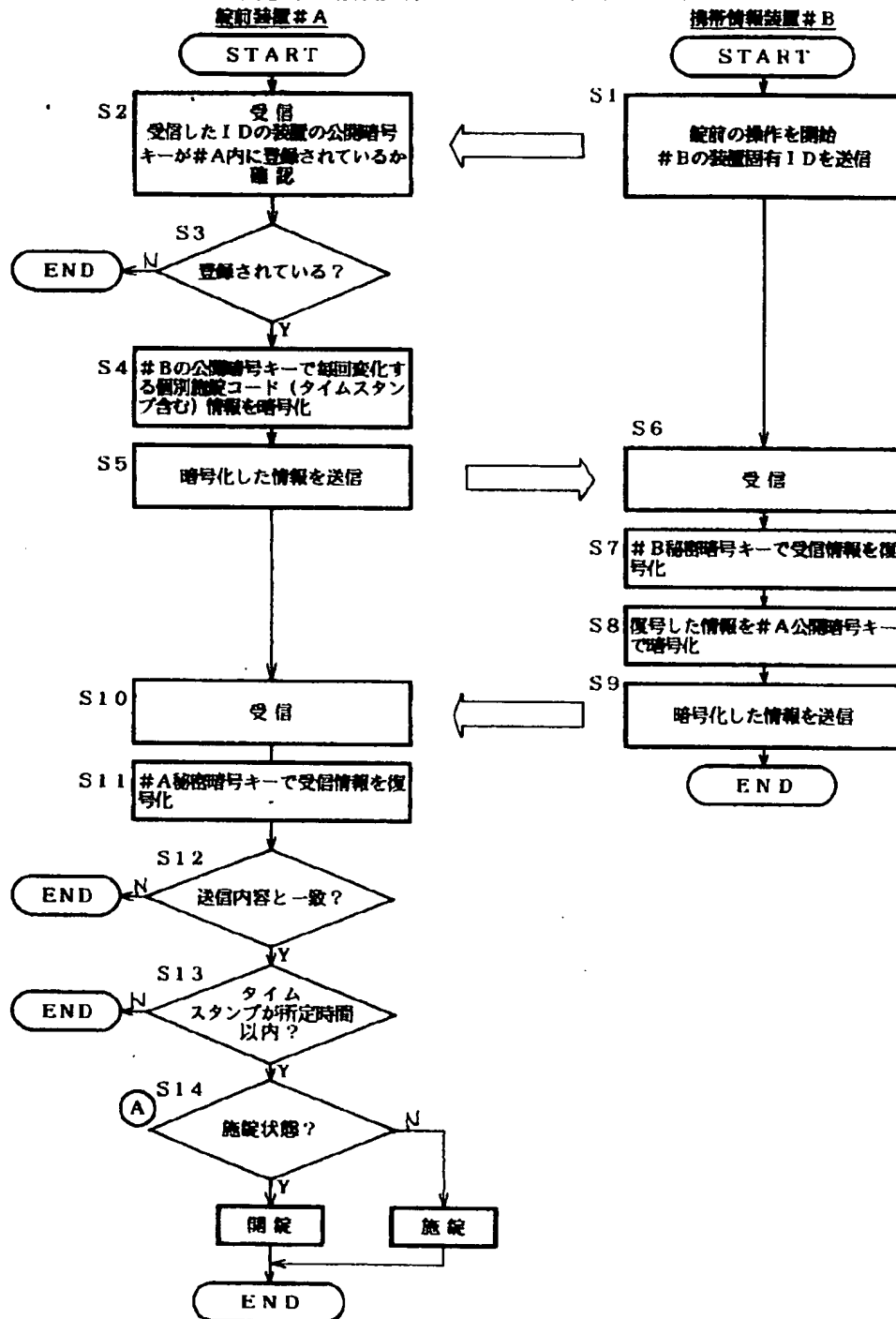
【図1】

本発明のシステム構成図



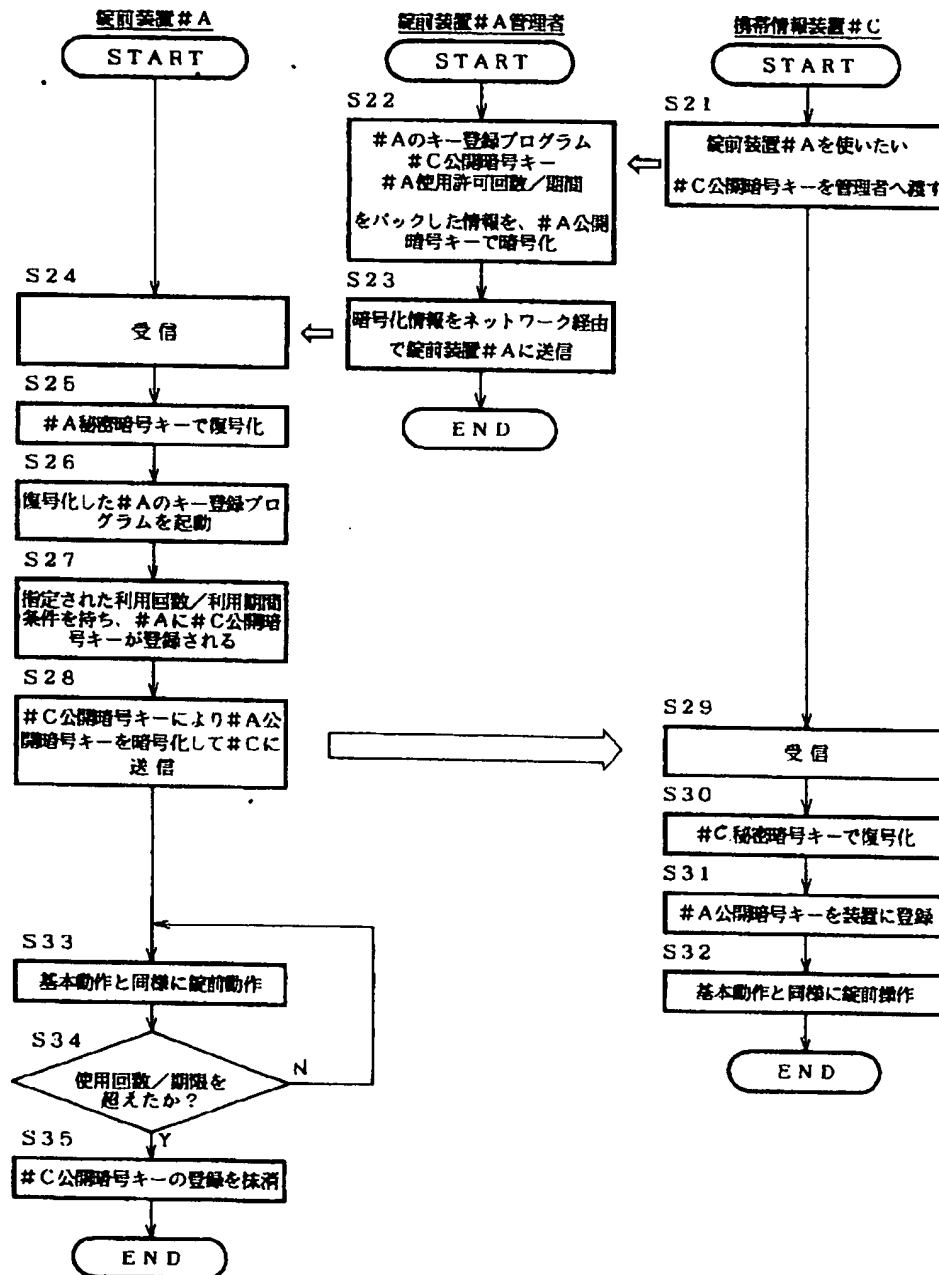
【図2】

本発明の動作説明フローチャート（その1）



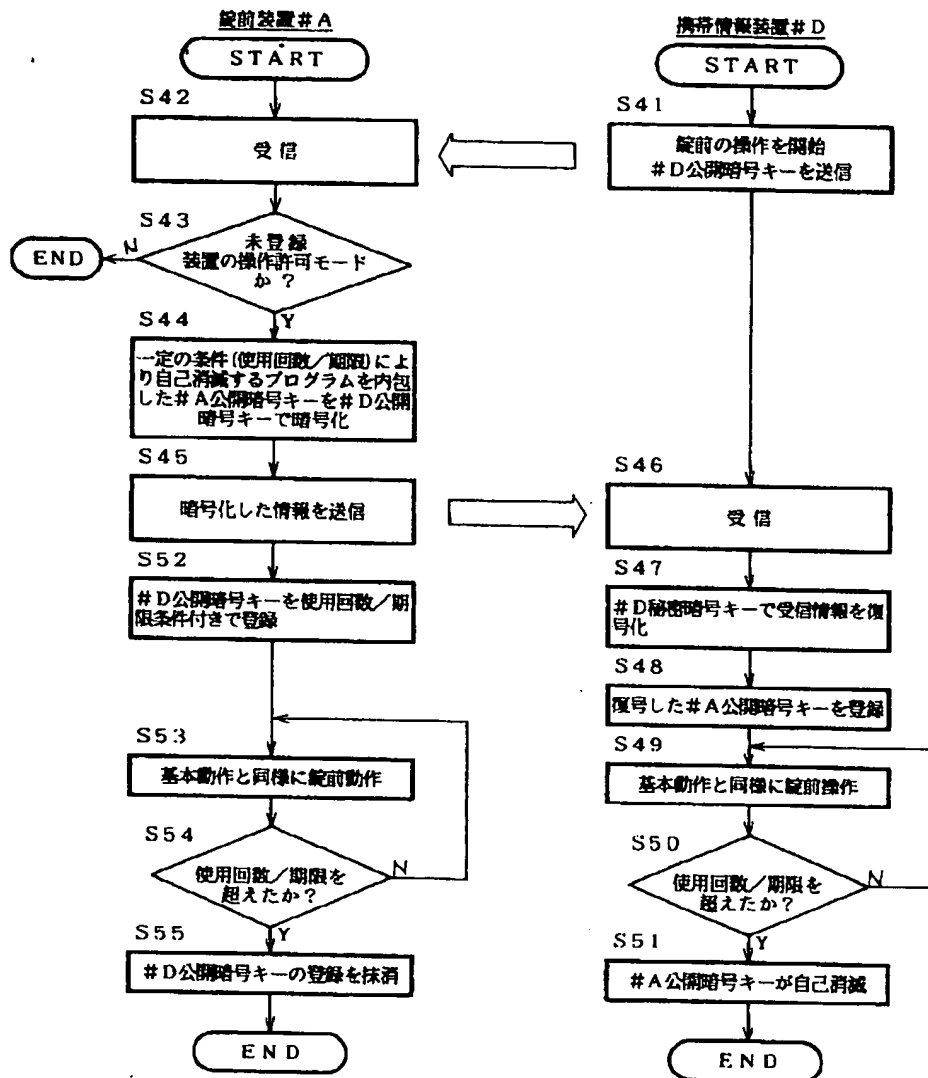
【図3】

本発明の動作説明フローチャート（その2）



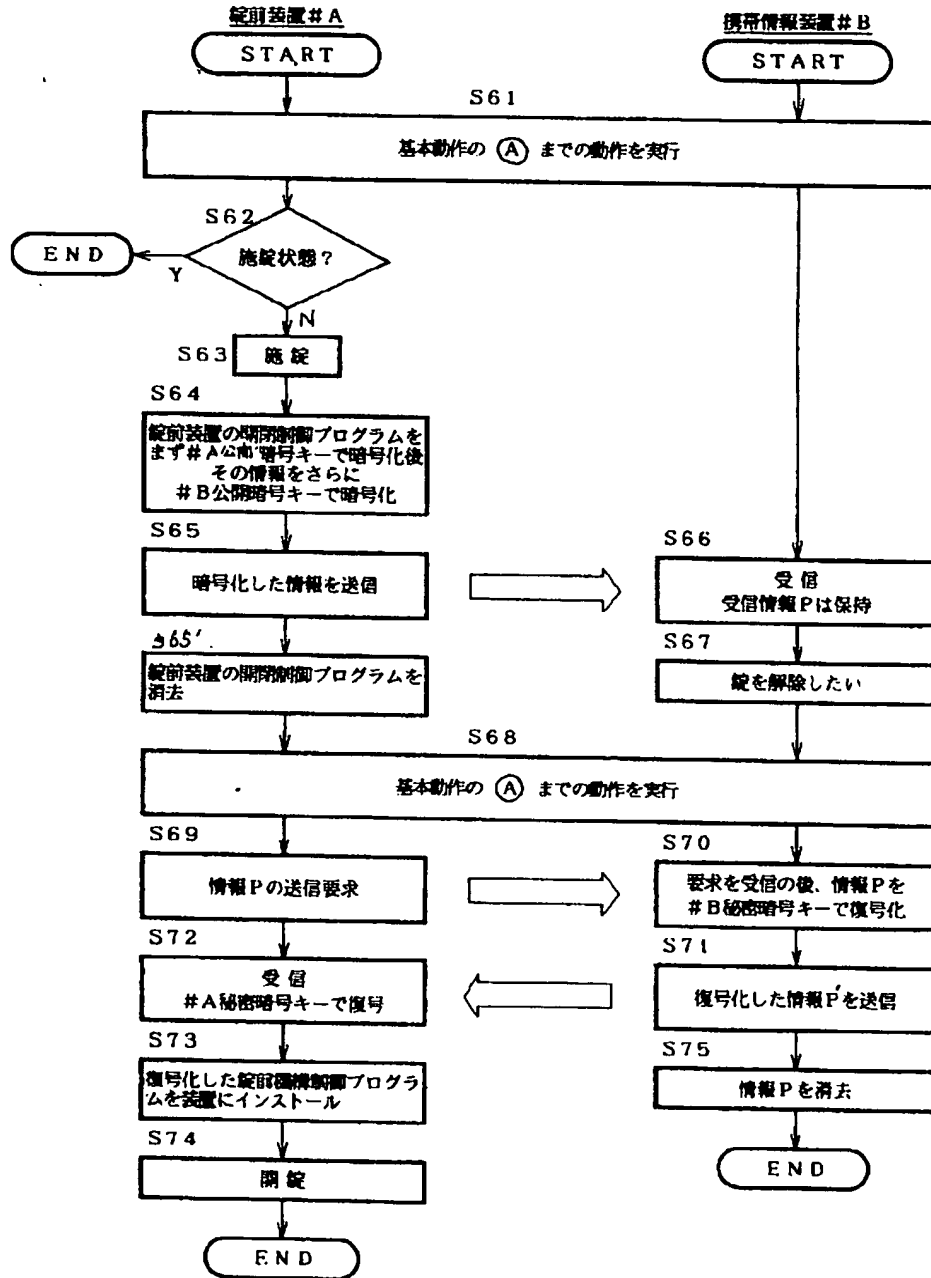
【図4】

本発明の動作説明フローチャート(その3)



【図5】

本発明の動作説明フローチャート(その4)



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.